MANAV RACHNA INTERNATIONAL INSTITUTE OF RESEARCH & STUDIES

Short Synopsis

For

Ph. D. Programme 2012-13

A NOVEL SECURITY MODEL BASED ON TRUST TO SECURE MOBILE AGENTS IN PRAXIS OF MOBILE ADHOC NETWORKS

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
FACULTY OF ENGINEERING & TECHNOLOGY

Submitted by:
Ms. Bindiya Bhatia
Registration No: 12/Ph.D/009
Email ID: bindiya.bhatia@gmail.com
Contact No.: 9910003764

Supervisor:
Prof (Dr.) M.K. Soni
Pro Vice Chancellor
Manav Rachna International Institute of Research & Studies, Faridabad
Email ID: pvc@mriu.edu.in
Contact No.: 9871588132

Joint-Supervisor:
Dr. Parul Tomar
Assistant Professor
Dept of Computer Engg.
YMCA University of Science & Technology, Faridabad
Email ID: ptomar_p@hotmail.com
Contact No.: 9818923336

ABSTRACT

Mobile Agents and Mobile Ad-hoc Networks are two different paradigms that when used together provide better interaction and communication. Although Mobile Ad-hoc Networks provide network formation to the areas where there is no infrastructure due to properties like self-formation, self-organization. But various challenges are also associated with mobile ad-hoc networks like dynamic topology, mobility, energy constraint etc. Various technologies and protocols are proposed to mitigate these issues. Mobile agent is one of the technologies. Mobile agents provide a new method of communication based on disconnected network which may result in efficient application development based on connectivity. Mobile agents travel in a network in a different and better way than conventional client-server architecture based applications. Features like mobility and autonomy enable an agent to accomplish several tasks in mobile ad-hoc networks like topology discovery, routing, key management, congestion control in an optimized manner. But everything comes with a price, as mobile agents are gaining reputation; they are more susceptible to threats. Malicious nodes in a network can reroute the agents, alter its code and data and even can kill it. Due to its major praxis in different fields, there are various security mechanisms to secure it. But all are not applicable in a resource-constraint environment like Mobile Ad-Hoc Networks due to its dynamic topology and lack of centralized entity. Mobile agents can be protected in Mobile Ad-Hoc Networks through cooperating behavior in which nodes co-operate and trust each other on the basis of some actions performed by mobile agents. The research work's includes intensive review of mobile agent's applications on several layers of mobile ad-hoc networks, existing security mechanisms to protect mobile agents, and role of trust to secure mobile agents. The major aim of research work is to provide energy efficient security model based on trust for the security of mobile agents when applied in MANET.

Key words: Mobile ad-hoc networks, mobile agents, security, routing, trust.

CONTENTS

S. No.	Description	Page No.
1	Introduction 1.1 Mobile Ad-hoc Network 1.2 Mobile Agents 1.3 Role of Mobile Agents in MANET 1.4 Security of Mobile Agents	1-4
2	Literature Review	4-6
3	Description of Broad Area	6-7
4.	Problem Identification and Objectives of the Study 4.1 Problems With the Existing Systems 4.2 Objectives of Study	7-8
5	Methodology	8
6	Expected outcome of the research	8-9
7	Proposed Time Frame	9
8	References	10-12

1. Introduction

Since many years, mobile computing is becoming popular with the increase usage of mobiles devices like Personal Digital assistant (PDAs), notebooks computers and smart phones. With the integration of computing devices with various mobile devices like phones, sensors, vehicles, military equipment etc, many new protocols and technologies are inventing to provide better communication and connectivity. Mobile Ad-Hoc Network (MANET) allows communication between mobile devices without any centralized entity (Kawaguchi, N., Toyama, K. and Inagaki, Y., 2000; Karlsson, J., Dooley, L.S. and Pulkkis, G., 2012). While MANET provides infrastructure-less and self-organizing network for communication, there are various issues associated with it like:

- Unpredictable network topology
- Mobility of nodes
- No Observable Boundaries
- Security
- Energy constraints
- Location aware routing
- Hidden Terminal Problem

Eminent Researchers worked to counter these issues and introduce new routing protocols and technologies. Further research is going on to optimize these algorithms and protocols used at different layers. And as a part of this research, a new technology is used at different layer of MANET to optimize various tasks like service discovery, network management, intrusion detection, routing, congestion control etc.

Mobile agents are small programs that can roam around a network from one device to another device autonomously, and also have the ability to communicate with their environment. Mobile agents provide better connectivity and communication as compared to client server paradigm. But the agents are vulnerable to threats due to their mobility. There are various security risks that are associated with mobile agents. This research work involves study a role of mobile agents in mobile ad-hoc networks, mobile agent security & improving the security of mobile agent used in MANET.

1.1 Mobile Ad-Hoc Networks

Mobile Ad-Hoc Network is a group of mobile devices with wireless communication. The device in a network has the ability to interact with each other without existence of any centralized entity. MANET is self-forming and self-organizing wireless network that can be dynamically formed to interchange information without using any fixed infrastructure (Al-Omari, and Sumari, 2010). In MANET, any node which can be mobile can enter in the network and connected dynamically. All nodes of this network can act as router and participate in route discovery and route maintenance. MANETs are flexible, provide low cost, and robust. Ad-hoc networks can be easily forms in the regions where proper infrastructure is not there or the cost of building the infrastructure is too high or when existing fixed infrastructure is not trustworthy, as in case of performing tasks related to military in the opponent zone. Ad hoc networks are also very beneficial in case of disasters, emergencies, conferences in which rapid information sharing is important. Because of node's mobility, network topology is subjective to change.

1.2 Mobile Agents

Mobile agents are innovative software programs which can travel from one device to another device, halting their execution and continuing where they halted on last device. While travelling from one device to another device, mobile agents can accumulate information from the devices (Manguer, 2003).

Mobile agents are not restricted to its owner node. Mobile agent has the ability to transfer itself from owner node to any another system in a network and communicate. Mobile agents are intelligently and autonomously choose their next destination themselves. They have the ability to take decisions autonomously. In order to accomplish any particular task, mobile agents travel around the network from one device to another device and can accumulate and disseminate the information. Mobile agents possess a feature that it can carry its code, execution state & data with itself to any of the node in the network. Due to which mobile agents can halt their execution on one node and can carry on its execution on the next visiting node from where it has halted execution on the previous device. It is able to transfer an incomplete transaction with itself when it travels from one device to another device and can complete that transaction on next

device where it will be transferred. Mobile agent consumes less bandwidth as compared to client-server applications.

1.3 Role of Mobile Agents in MANET

Mobile agents are being used in various fields of MANETs like topology discovery, key management, routing, security, congestion control. With the use of mobile agents the load on the network can be reduced due to their asynchronous behaviors as compared with the traditional technologies used in these areas. Mobile agents were introduced in Mobile ad-hoc network by MIT Media Lab (Minar et. al., 1999) for routing purpose. Migas et. al. (2003) worked towards a problem of delay in route discovery and presented the perception of mobile agents to find the best path. Marwaha et. al. (2002) introduced Ant-AODV routing protocol based on mobile agents which is a combination of ant-based routing and AODV routing protocols. Roy Choudhury et. al. (2000) designed an application based on mobile agents for making the nodes in the network topology aware. Mobile agents are also used for congestion control (Sharma and Bhadauria, 2011) and key management (Zhang et. al. 2009; Pushpa Lakshmi and Kumar, 2010) in a network. Many intrusion detection systems are also designed based on mobile agents (Zhang and Lee, 2000; Rizvi et. al., 2010).

Although mobile agent is a virtuous solution to resolve various issues arises in the several fields of MANET, still security of mobile agents is a big concern. Mobile agents are susceptible to various security risks. Our research work's main aim is to address the existing security issues and provide an efficient security mechanism to secure mobile agents used in MANET.

1.4 Security of Mobile agents in MANETs

According to Kumar (2010) security threats of mobile agents can be categorized as:

- Threat from mobile agent to mobile agent: Any mobile agent can access and alter another mobile agent's code and data by invoking the public methods of another agent. Also the threats of masquerade, repudiation and denial of services are also there.
- Threat from mobile agent to host: Various threats are there from mobile agents to host as mobile agents can access the methods and data of host on order to complete any transaction, it can harm the host by using excess amount of resources of host leading to denial of services.

- Threat from host to mobile agent: If the visiting node is harmful, it can harm the agent by rerouting it, altering its code and data and killing it.

Lot of research work is reported to address the security issue of mobile agents. But all the techniques are not suitable and applicable to provide security to mobile agents when praxis in Mobile Ad-Hoc Networks because of the limited resources like bandwidth, energy and lack of centralized entity. The next section presents the existing security mechanisms.

2. Literature Review

A lot of research work has been done to protect Mobile Agent. Some mechanisms are proposed to protect only the code and some are to protect the host platforms from malicious mobile agents. Some of the existing works are discussed below:

Askwith et. al. (1997) introduced location privacy of the mobile users through smart cards. In the scheme, mobile users can register themselves to a local network through smart card. This smart card contains the personal information of the user. The local network can further interact with home network without indicating the location of the user and thus the user's location remain unidentified. Scheme uses digital mix for the communication between local network and home network. Scheme provides only location privacy to mobile users.

D'Anna et. al. (2003) proposed a technique named obfuscation in which mobile agent's code and state is preserved through obfuscated code. Obfuscation program inputs the mobile agent's code and state and provide obfuscated code which can be run on different host platforms. This prevents the mobile agent's code and data being analyzed. This scheme provides the security to mobile agents.

Pushpa Lakshmi and Kumar (2010) have proposed the sandboxing technique to secure visiting host from harmful mobile agents. The visiting host provides full access to the local code which can access all the resources of the system. But the remote code like mobile agents, applets are restricted to be executed in a restricted area called sandbox which provide limited access to the remote code.

Lee and Necula (1997) introduced the *Proof-Carrying Code* (PCC) technique in which the owner of the mobile agent provides a formal proof that the mobile agent's code complies with the security policy of the visiting node. The mobile agents are sent with the formal safety proof to

the visiting node. The visiting node verifies these safety proofs by using a fast proof checker which provides reasoning to some inference rules. If the proof checkers approves the safety proofs, then the mobile agent can be executed on the host platform.

Chaum (1985) proposed the concept of digital mix which provides privacy in terms of location and content. In this technique, two nodes can communicate with each other without knowing the content of mobile agent and location of each other through intermediate node which is called 'mix'.

Farmer et. al. (1996) introduced the "State Appraisal" mechanism which preserves the state of mobile agent against any alteration or medication by malicious node. The owner node builds a state appraisal function along with agent which comprise of set of permissions that an agent could request at the visiting node. The scheme is only dedicated to secure agent's state.

Sultanik et. al. (2003) introduced a technique of Threshold Cryptography to secure mobile agents and hosts against possible threats. The technique uses the concept of signing a certificate through a pair of public and private key. The certificate is signed through master public key which is known to all the nodes. The private Key is distributed into a no. of shares and each share is kept on different node in a group. For decryption of agent on the visiting host, the visiting host requires the all shares of private key for the complete formation of the key. But there is a possibility of non-availability of the node having the share of private key due to mobility of the node.

Ahmed (2009) proposed a concept of a Secure Image Controller (SIC). The SIC build an image of the mobile agent and send it to the visiting host before sending the original agent. After receiving the image back, it is compared with the original agent. If the image is same, it shows that there is no alteration on the code and data and the host is secure enough to interact. And the original agent is sent to communicate. This proposed technique not works well in MANET due to bandwidth requirement and use of third party SIC which can be a bottleneck in MANET.

Borselius (2002) proposed the method to authenticate and authorize a mobile agent through digital signatures. The mobile agents are digitally signed by the owner node before sending it to the visiting node which provides proper authentication of the mobile agent. The scheme

provides security to mobile agents but is not applicable to MANET due to central certificate authority.

Haghighat and Yarahmadi (2008) proposed a technique with three agents. The first agent is called the dummy agent which is sent to the host first with dummy data. If the host is malicious and harms the dummy agent by altering its data or killing it then the source node will get to know and will not send the original data. If host finds no alteration in dummy agent, then host record the path of the destination node through second agent which is record agent. Afterward third agent which is the original agent is sent to the host with original data. But scheme is not suitable to MANET because it requires lot of bandwidth which is expensive in MANET.

Geetha and Jayakumar (2011) proposed Trust enhanced symmetric key cryptography. A centralized entity is used to implement knowledge based system (KBS) and provides the identity information of the trusted hosts. The scheme is not suitable in MANET due to the use of trusted third party which is centralized entity.

As appear from the literature that very few works address the entire security aspects of mobile agent system in a mobile ad hoc network. Also very less attention has been reported towards the consideration of the effect of security computations on battery power of the mobile node. This becomes the motivation towards further research to propose an efficient security mechanism to provide security to mobile agents as well host while considering the energy level of the node.

3. Description of Broad Area

Nowadays mobile agent seems to be a popular choice to perform various functions like topology discovery, network management, congestion management, key management, routing, automatic network reconfiguration etc. for resource-constrained environments like mobile ad-hoc networks. Many a time task processing is taken up by mobile agents that travel in the network and get the task done.

But securing mobile agents is a big concern particularly when the network usually undergoes continuous topology changes. Mobile agent security stresses on securing a mobile agent which is vulnerable to various attacks through malicious hosts by applying cryptographic functions or other mechanisms. There are lots of security approaches to secure mobile agents as mentioned in

literature review section. Some uses cryptographic functions to provide authenticity, data integrity and non-repudiation (Shrivastava and Mehta, 2012; Geetha and Jayakumar, 2011; Sultanik et. al, 2003). Some uses trust (Chowdhury and Neogy, 2011) to prevent attacks like blackhole and warmhole. But still lots of problems exist with the present security approaches.

4. Problem Identification and Objectives of Study

This section is describing the unsolved problems with the existing security techniques and further objectives of the research.

4.1 Problems with the Existing Systems

There are lot of unsolved problems, challenges and issues with the existing system and few needs more improvisation. Some of the issues are mentioned below:

- The existing approaches either consider the attacks by hosts or attacks by agents, but don't provide security to host and agent both as a complete security solution.
- Very few of the existing approaches considered the constraint of limited battery power of a node in MANET.
- Only few technologies provide security to mobile agent state and protection of mobile code against input and output analysis.

4.2 Objectives of Research

Very few of the existing technologies have taken battery constraint of the node in to consideration while giving solutions to provide security to the mobile agents in MANET. This research work aims to consider battery constraint of the mobile node while providing complete security solution in terms of protecting host and mobile agents in MANET. The objectives of the study are:

- To review the current security solutions for mobile agents in MANET.
- To identify the parameters those are affected while giving the security solutions.
- To simulate the existing technologies without and with considering the energy level of the node.

- To develop and design an improved security mechanism to protect mobile agents as well as host while considering the energy level of the node.
- To simulate the proposed improved security mechanism considering the battery level of the node and evaluate on the basis of performance parameters like packet delivery ratio, throughput, energy consumption.

The research work will consolidate major issues, merits and demerits of the existing technologies. The work will provide better awareness about current security solutions for mobile agents, issues in these technologies and may propose a framework to provide complete security mechanism considering the battery constraint of mobile node.

5. Methodology

The methodology of the research work would be carried out in phases to obtain the main objectives of the research. The phases of the research work are given below:

Phase1: Literature Review

Phase 2: Comparing and evaluating merits and demerits of the existing mechanisms which are providing security to the mobile agents in MANETs and to identify the areas for improvisation.

Phase 3: Formulating the research objectives-The problem statement

Phase 4: Identifying the available tools to simulate the existing security mechanism and developing better solution.

Phase 5: Design and development of an improved security mechanism in a simulated environment to secure the mobile agents.

Phase 6: Research Publications, writing of thesis and submission.

6. Expected Outcome of the research

The research work will provide insight knowledge of the current security mechanisms for mobile agents. It also helps to compare the different mechanism and their merits and demerits. It also helps to give knowledge about the various tools used to simulate mobile agent and mobile ad-hoc

network. The research work will come out with an efficient security mechanism for mobile agents in MANETs considering the energy constraint of the mobile nodes in MANETs.

7. Proposed Time Frame

	Sem 1 & sem 2 (Jan '13 - Dec 2013)	Sem 3 (Jan '14- June '14)	Sem 4 (July '14- Dec '14)	Sem 5 (Jan '15 - June '15)	Sem 6 (July '15 – Dec '15)	Sem 7 (Jan '16 – June '16)	Sem 8 (July '16- Dec '16)	Sem 9 (Jan '17 – Dec '17)	Sem 10 (Jan '18 – June '18)
Course work									
Literature review									
Problem Formulation									
Implementation									
Testing and Analysis									
paper presentation and publication									
Thesis Writing & Submission									

References

- Ahmed, T.M., 2009. Using secure-image mechanism to protect mobile agent against malicious hosts. *World Academy of Science, Engineering & Technology, International Journal of Computer and Information Engineering*, 3(11), pp.439-444.
- Al-Omari, S.A.K. and Sumari, P., 2010. An overview of mobile ad hoc networks for the existing protocols and applications. *Journal on Application of Graph Theory in Wireless Ad-Hoc Network & Sensor Network*, 2(1), pp. 87-110.
- Askwith, B., Merabti, M., Shi, Q. and Whiteley, K., 1997, December. Achieving user privacy in mobile networks. In *Computer Security Applications Conference, 1997. Proceedings., 13th Annual* (pp. 108-116). IEEE.
- Borselius, N., 2002. Mobile agent security. *Electronics & Communication Engineering Journal*, *14*(5), p.211-218.
- Chaum, D., 1985. Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, *28*(10), p.1030-1044.
- Chlamtac, I., Conti, M. and Liu, J.J.N., 2003. Mobile ad hoc networking: imperatives and challenges. *Ad hoc networks*, *1*(1), pp.13-64.
- Chowdhury, C. and Neogy, S., 2011. Securing Mobile Agents in MANET against attacks using Trust. *International Journal of Network Security & Its Applications*, *3*(6), p.259 - 274.
- D'Anna, L., Matt, B., Reisse, A., Van Vleck, T., Schwab, S. and LeBlanc, P., 2003. Self-protecting mobile agents obfuscation report. *Network Associates Laboratories Report*.
- Farmer, W.M., Guttman, J.D. and Swarup, V., 1996, September. Security for mobile agents: Authentication and state appraisal. In *European Symposium on Research in Computer Security* (pp. 118-130). Springer, Berlin, Heidelberg.
- Geetha, G. and Jayakumar, C., 2011. Trust enhanced data security in free roaming mobile agents using symmetric key cryptography. *International Journal of Network Security & Its Applications*, *3*(5), p.217 - 228
- Haghighat, R. and Yarahmadi, H., 2008. A New Approach for Mobile Agent Security. *The Proc. of the World Acadamy of Science, Engineering and Technology*, *32*. P. 717-720

- Hohl, F., 1998. Time limited blackbox security: Protecting mobile agents from malicious hosts. In *Mobile agents and security* (pp. 92-113). Springer, Berlin, Heidelberg.
- Karlsson, J., Dooley, L.S. and Pulkkis, G., 2012. Routing security in mobile ad-hoc networks. *Issue Inform. Sci. Inform. Technol*, *9*, pp.369-383.
- Kawaguchi, N., Toyama, K. and Inagaki, Y., 2000. MAGNET: ad hoc network system based on mobile agents. *Computer Communications*, *23*(8), pp.761-768.
- Kumar, S.A., 2010. Classification and review of security schemes in mobile computing. *Wireless Sensor Network*, *2*(06), p.419-440
- Lee, P. and Necula, G., 1997, March. Research on proof-carrying code for mobile-code security. In *DARPA workshop on foundations for secure mobile code* (pp. 26-28). United States Department of Defense, Defense Advanced Research Projects Agency (DARPA) Pittsburgh, PA, USA.
- Manguer, A., 2003. *Mobile agents in ad hoc networks* (Doctoral dissertation, thesis, April).
- Marwaha, S., Tham, C.K. and Srinivasan, D., 2002, November. Mobile agents based routing protocol for mobile ad hoc networks. In *Global Telecommunications Conference, 2002. GLOBECOM'02. IEEE* (Vol. 1, pp. 163-167). IEEE.
- Migas, N., Buchanan, W.J. and McARTNEY, K.A., 2003, April. Mobile agents for routing, topology discovery, and automatic network reconfiguration in ad-hoc networks. In *Engineering of Computer-Based Systems, 2003. Proceedings. 10th IEEE International Conference and Workshop on the* (pp. 200-206). IEEE.
- Minar, N., Kramer, K.H. and Maes, P., 1999. Cooperating mobile agents for dynamic network routing. In *Software agents for future communication systems* (pp. 287-304). Springer, Berlin, Heidelberg.
- Pushpav Lakshmi, R. and Kumar, A.V.A., 2010. Cluster based composite key management in mobile ad hoc networks. *International Journals of Computer Applications 4(11)*, p.30-35.
- Rizvi, S.M.S.I., Sultana, Z., Sun, B. and Islam, M.W., 2010. Security of mobile agent in ad hoc network using threshold cryptography. *World Academy of Science, Engineering and Technology*, *30*, pp.424-427.

- Roy Choudhury, R., Bandyopadhyay, S. and Paul, K., 2000, November. A distributed mechanism for topology discovery in ad hoc wireless networks using mobile agents. In *Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing* (pp. 145-146). IEEE Press.
- Sharma, V.K. and Bhadauria, S.S., 2011. Agent based congestion control routing for mobile ad-hoc network. In *Trends in network and communications* (pp. 324-333). Springer, Berlin, Heidelberg.
- Shrivastava, R. and Mehta, P., 2012. Analysis of Secure Mobile Agent System. *International Journal of Soft Computing and Engineering (IJSCE) ISSN*, pp.2231-2307.
- Sultanik, E., Artz, D., Anderson, G., Kam, M., Regli, W.C., Peysakhov, M., Sevy, J., Belov, N., Morizio, N. and Mroczkowski, A., 2003, August. Secure Mobile Agents on Ad Hoc Wireless Networks. In *IAAI* (pp. 129-136).
- Wahbe, R., Lucco, S., Anderson, T.E. and Graham, S.L., 1994, January. Efficient software-based fault isolation. In *ACM SIGOPS Operating Systems Review* (Vol. 27, No. 5, pp. 203-216). ACM.
- Zhang, Y. and Lee, W., 2000, August. Intrusion detection in wireless ad-hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking* (pp. 275-283). ACM.
- Zhang, Y., Zhu, L.N. and Feng, L., 2009. Key Management and Authentication in Ad Hoc Network based on Mobile Agent. *Journal of Networks*, *4*(6), p.487-494.